

## МЕДИЧНА ІНФОРМАТИКА ТА ІНЖЕНЕРІЯ

УДК: 61 : 651. 928: 681. 3І: 003.26 : 681. 3І: 007

### МАТЕМАТИЧНІ АЛГОРИТМИ ЗАХИСТУ ІНФОРМАЦІЇ

**І. М. Шупяцький**

*Державна служба спеціального зв'язку та захисту інформації України*

У статті проаналізовано математичні алгоритми захисту інформації з метою використання методології алгоритму криптографії в медицині.

**Ключові слова:** криптографія, алгоритм, ключ, методологія.

### МАТЕМАТИЧЕСКИЕ АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ

**И. М. Шупяцкий**

*Государственная служба специальной связи и защиты информации Украины*

В статье проанализированы математические алгоритмы защиты информации с целью использования методологии алгоритма криптографии в медицине.

**Ключевые слова:** криптография, алгоритм, ключ, методология.

### MATHEMATICS ALGORITHMS OF THE INFORMATION PROTECTION

**I. M. Shupiatyskyi**

*State department of the special connect & protection information of Ukraine*

There were discussed mathematics algorithms of the information protection with purpose to use the main methods of the cryptography algorithm in the medicine.

**Key words:** cryptography, algorithm, key, main methods.

*Присвячується 120-річчю засновника сучасних математичних методів криптографії, академіку АН УРСР М. П. Кравчуку.*

**Вступ.** На сьогодні захист інформації здійснюється за допомогою та на основі сучасних техніко-економічних криптографічних засобів. Медична інформація - це інформація конфіденційна, яка потребує цілеспрямованого захисту, захисту криптографічного в сучасному інформаційному просторі. Мета захисту - недопущення використання медичної інформації особами, які не мають права доступу до конфіденційних ресурсів.

Одним із основних методів сучасних криптографічних алгоритмів є прикладна теорія чисел, яка є фундаментом сучасних математичних криптографічних алгоритмів. При обміні інформацією між учасниками часто виникає ситуація, коли інформація не є конфіденційною, а саме, - отримання повідомлень у неперекрученому вигляді і наявність гарантії, що ніхто не в змозі підробити повідомлення.

**Мета роботи** полягає в проведенні аналізу математичних алгоритмів захисту інформації для можли-

востей використання методології алгоритму криптографії в медицині.

**Отримані результати та їх обговорення.** Криптосистеми із секретним ключем (одноключові, симетричні або класичні), а також криптосистеми з відкритим ключем (асиметричні) максимально адаптовані до використання з метою захисту і збереження інформації. Як приклад можна навести основні положення криптологічного протоколу "електронний підпис".

Математична криптографія виникла як наука про шифрування інформації, - як наука про криптосистеми. Криптосистема без передачі ключів.

Абоненти А, В, С, ... домовились організувати закриті листування між собою. Для цього вони вибрали достатньо велике просте число  $p$  і таке, що  $p-1$  добре розкладається на не дуже великі прості множники. Якщо серед множників такого числа кратних немає, то число  $p-1$  називають Евклідовим. Кожний з абонентів, незалежно один від одного, вибирає випадкове число, натуральне, взаємно просте з числом  $p-1$ : А, В, С, ... - абоненти; а, б, с, ... - вибрані ними

випадкові числа. В подальшому абонент А знаходить число  $\alpha$  з умов

$$a \cdot \alpha \equiv 1 \pmod{\phi(p)}, 0 < \alpha < p-1; \quad (1)$$

абонент В знаходить число  $\beta$  з умови

$$b \cdot \beta \equiv 1 \pmod{\phi(p)}, 0 < \beta < p-1, \quad (2)$$

де  $\phi(p)$  - функція Ейлера,  $a, \alpha$  - закриті ключі абонента А;  $b, \beta$  - закриті ключі абонента В тощо.

У тому випадку, коли абонент А вирішує надіслати повідомлення  $t$  абоненту В можна прогнозувати, що  $0 < m < p-1$ . Тоді він спочатку зашифрує це повідомлення своїм першим закритим ключем, знаходить:

$$m_1 \equiv m^a \pmod{p}, 0 < m_1 < p \quad (3)$$

і направляє абоненту В. Абонент В, в свою чергу, зашифровує знову це повідомлення також своїм першим ключем:

$$m_2 \equiv m_1^b \pmod{p}, 0 < m_2 < p \quad (4)$$

і пересилає його у зворотному напрямку абоненту А. Абонент А, отримавши своє подвійно зашифроване повідомлення, шифрує його ж втретє своїм другим ключем:

$$m_3 \equiv m_2^a \pmod{p}, 0 < m_3 < p \quad (5)$$

і знову відправляє його абоненту В. Останній розшифровує цю шифротелеграму за допомогою свого другого ключа:

$$m_4 \equiv m_3^b \pmod{p}, 0 < m_4 < p.$$

Таким чином, з порівняння (3) - (4) маємо:

$$m_4 \equiv m^k \pmod{p},$$

$$\text{де } k \equiv a \cdot \alpha \cdot b \cdot \beta \pmod{p-1}.$$

В силу (1) і (2)  $k \equiv 1 \pmod{\phi(p)}$ . Тому  $m_4 \equiv m \pmod{p}$  а так як кожне з них позитивне і менше  $p$ , то  $t_4 = t$ .

Наприклад, нехай абоненти А і В вирішили встановити між собою прихований зв'язок без передачі ключів. Вони вибрали для цього просте число  $p = 9551$ . Тоді  $p-1=9550$ .

Абонент А вибирає випадкове число  $\alpha=8159$ , а абонент В -  $b=7159$ . Абонент А вирішує рівняння:  $8159 \cdot \alpha \equiv 1 \pmod{\phi(9551)}$ ,  $0 < \alpha < 9550$  й знаходить  $\alpha=6639$ , а абонент В вирішує рівняння:  $7159 \cdot \beta \equiv 1 \pmod{\phi(9551)}$ ,  $0 < \beta < 9550$  й знаходить  $\beta=6139$ .

Абонент А вирішує надіслати секретне повідомлення абоненту В  $t=7032$ . Тоді він спочатку шифрує повідомлення своїм першим ключем:  $m_1 \equiv m^a \pmod{p} = 7032^{8159} \pmod{9551} = 153$ .

Абонент В, отримавши це повідомлення, шифрує його своїм першим ключем:  $m_2 \equiv m_1^b \pmod{p} = 153^{7159} \pmod{9551} = 4896$ , і пересилає його абоненту

А, який, отримавши зашифроване повідомлення, шифрує його ж в третій раз своїм другим ключем:  $t_3 \equiv t_2^a \pmod{p} = 4896^{6639} \pmod{9551} = 7577$  і відправляє його абоненту В, який розшифровує цю шифротелеграму за допомогою свого другого ключа:  $t_4 \equiv t_3^b \pmod{p} = 7577^{6139} \pmod{9551} = 7032$ .

Розглянемо схожий приклад, але з великими числами, а саме нехай абоненти А і В вибирають випадкове число  $p = 3\ 618\ 502\ 788\ 666\ 131\ 106\ 986\ 593\ 281\ 521\ 497\ 1204\ 1468\ 702\ 080\ 126\ 762\ 623\ 304\ 9500\ 247\ 285\ 301\ 313$ . Далі абонент А вибирає випадкове число  $a=32910091146\ 424120843099383651147010\ 09965471731267159726697218119$ , а абонент В -  $b=7\ 213\ 345\ 672\ 919\ 431\ 2009114642445656781208430\ 934647938365165454\ 65843$ . Абонент А вирішує рівняння:  $3291009114642412084309938365114701009965\ 4717312671\ 59726697218119 \cdot a \equiv 1 \pmod{\phi(361850278\ 866613110698659328152149712041468702080\ 1267626233049500247285301313)}$ ,  $0 < a < 3618502\ 788\ 666131106986593281521497120414687020801267626\ 233049500247285301312$  і знаходить  $a=7182890\ 94672427671226754071206041429575840582\ 862\ 25696133\ 69504272231654775$ , а абонент В вирішує рівняння:  $721334567291943120091146\ 42445656781\ 20843093464793836516545465843 \cdot b \equiv 1 \pmod{\phi(119726\ 2141301475670592458614961179049\ 70213993920\ 59391)}$ ,  $0 < b < 119726214130\ 1475670592458614961179\ 049702139939205\ 9390$  і знаходить  $b=205078500\ 8947982616772154473648909901784058010689679\ 595249365486507640220987$ .

Абонент А вирішує надіслати секретне повідомлення абоненту В  $t=1643953085623702335973\ 4047455621923453212389086$ . Тоді він спочатку шифрує повідомлення своїм першим ключем:  $t_1 \equiv m^a \pmod{p} = 164395308\ 56237023359734047455621\ 92345321\ 2\ 3\ 8\ 9\ 0\ 8\ 6\ 3291009114642412084309938365114701009965\ 471731267159726697218119 \pmod{36185027886661311069865\ 93281521497120414687020801267626233049500247285\ 301313} = 23404884717260896071245567562641693\ 3820229094970133\ 5616973062664572414115995$ .

Абонент В, отримавши це повідомлення, шифрує його своїм першим ключем:  $m_2 \equiv m_1^b \pmod{p} = 23404884717260896071245567562641693382022\ 90949\ 70133561697306266457241411599572133456729194312009114642445656781208430934\ 64793836516545465843 \pmod{36185027886661311069865\ 9328152149712041468702\ 080126762623\ 304950024728\ 5301313} = 200847152309106133691890020899\ 385\ 1807662985672512619192514870979350742436070$ , і пересилає його абоненту А. Абонент А, отримавши зашифроване повідомлення, шифрує його ж в третій раз своїм другим ключем:  $m_3 \equiv m_2^a \pmod{p}$

=2008471523091061336918900208993851 8076629  
85672512619192514870979350742436070<sup>7182890</sup>  
9467242767122675407120604142099575840582862256961336950427231654775(mod

361850278866613110698659328152149712041468  
7020801267626233049500247285301313)=337426795  
6 0 6 6 4 0 4 4 9 1 4 4 3 9 6 3 9 2 1 3 5 6 2 0 3 6 4 9  
752330364752225196611392536160948437196 і  
відправляє у зворотньому напрямку його абоненту  
В, котрий розшифровує цю шифротелеграму за до-  
помогою свого другого ключа:  $m_4 \circ m_3^b \pmod p =$   
33742679560664044914439639213562036497523  
30364752225196611392536160948437196<sup>20507850089479</sup>  
82616772154473648909901784058010689679595249365486507640220987

(mod 3618502788666131106986593281521497120414  
687020801267626233049500247285301313)=  
16439530856237023359734047455621923453212389086

Прикладом можуть служити паперові купюри. Як що  
ресурсом є деякий товар, то наявність у покупця дос-  
татньої кількості купюр є доказом його права на доступ  
до ресурсу. З іншої сторони, хоча кожна паперова купю-

ра і має унікальний номер, відслідкувати купюри за но-  
мерами та виявити, хто її використав і в яких платежах,  
практично неможливо.

**Висновки.** 1. Для запобігання загрози контролю  
за джерелами інформації (звідки пересилаються по-  
відомлення) необхідна система контролю за досту-  
пом до ресурсів, яка повинна задовольняти двом,  
здавалося б, взаємно протилежним потребам.

2. Кожен бажаючий повинен мати можливість звер-  
нутися до цієї системи анонімно, при цьому все ж  
довівши своє право на доступ до ресурсів.

3. Якщо задача забезпечення конфіденційності ви-  
рішується за допомогою криптосистем, то для за-  
безпечення цілісності і унеможливлення відслідко-  
вування розробляють криптографічні протоколи.  
Адаптація криптографічних алгоритмів до телеме-  
дицини дасть можливість впровадження нових нау-  
кових та практичних досягнень, продуктом яких слід  
очікувати телемедичний алгоритм в криптографії, де  
осовою є поліном М. П. Кравчука.

#### Література.

1. Анализ современных зарубежных систем защиты информации / под ред. В. Ф. Колчина. // Обозрение прикл. и промышл. матем. - 2000. - Т. 7.
2. Вероятностно-статистический анализ последовательностей над конечным алфавитом / под ред. В. Г. Михайлова, В. П. Чистякова. // Обозрение прикл. и промышл. матем. - 1995. - Т. 2.
3. Конечные автоматы: прообразы выходных последовательностей над конечным алфавитом / под ред. В. Г. Михайлова, В. П. Чистякова. // Обозрение прикл. и промышл. матем. - 1995. - Т. 1.
4. Методы дискретной теории вероятностей / под ред. А. М. Зубкова. // Обозрение прикл. и промышл. матем., 1996, т. 3. в. 4.
5. Новые подходы к решению вероятностных задач. Под ред. А. М. Зубкова. // Обозрение прикл. и промышл. ма-

тем.. - 1994. - Т. 1, В. 4.

6. Пороговая логика и нейрокомпьютеры. / под ред. Г. В. Балакина. // Обозрение прикл. и промышл. матем. - 1994. - Т.1, В. 3.

7. Браун П. Приватность в век терабайтов и терроризма / Питер Браун // В мире науки. - 2008. - №> 12. - С. 20-21.

8. Ванчаков Н. Б. Практические основы защиты информации. Технические методы и средства : производственно-практическое издание / Н. Б. Ванчаков, А. Н. Григорьев. - Калининград : КЮИ МВД России, 2000. - 198 с.

9. Голубев Д. Л. Распределенные центры обработки данных / Голубев Д. Л. // Jet Info. - 2006. - №> 5. - С. 3-16.

10. Горбатов В. С. Основы технологии РКІ / В. С. Горбатов, О.Ю. Полянская. - М. : Горячая линия - Телеком, 2004 - 246 с.